

**AFFIDAVIT IN SUPPORT OF**  
**AN APPLICATION FOR SEARCH WARRANTS**

I, Mary Behler, a Special Agent with the United States Bureau of Alcohol, Tobacco, Firearms & Explosives ("ATF"), being duly sworn, depose and state as follows:

**INTRODUCTION**

1. I am a Special Agent with ATF, and have been so employed since December 2013. Prior to becoming a Special Agent with ATF, I was a Federal Air Marshal with the Federal Air Marshal Service ("FAMS") – from November 2010 through December 2013. I completed the Federal Law Enforcement Basic Training Course in Artesia, New Mexico, the Federal Air Marshal Basic Training Academy in Atlantic City, New Jersey, the Criminal Investigator Training Program in Glynco, Georgia, and the ATF Special Agent Basic Training at the Federal Law Enforcement Training Center in Glynco, Georgia. I also obtained an Undergraduate Degree in Criminal Justice and a Master's Degree in Law Enforcement Intelligence Analysis from Michigan State University. I have received firearms, arson, and explosives related training and I have utilized a variety of investigative techniques and resources, including physical and electronic surveillance and various types of cooperating sources in order to successfully conduct these investigations. Further, I have received periodic training in the fields of firearms, narcotics, arson and explosives investigation.

2. As an ATF Special Agent, I conduct investigations involving violations of Federal firearms laws. During my service with ATF, I have conducted numerous criminal investigations involving the illegal possession of firearms and the intrastate, interstate, and international trafficking of firearms. Further, I also have experience investigating offenses involving explosive devices. As a federal agent, I am authorized to investigate violations of United States laws and to execute search warrants issued under the authority of the United States.

**IDENTIFICATION OF THE ITEMS TO BE SEARCHED**

3. This affidavit is made in support of an application pursuant to Rule 41 of the Federal Rules of Criminal Procedure for:

- a. a search warrant authorizing a search of one Gateway desktop computer, Model No. SX2110G, Serial No. DTGDYAA0022460790B9200, SNID 24603098792, which was recovered earlier today during the execution of a search warrant signed yesterday by this Court, from the residence of Keith Seppi at 716 Middle Road, Conneaut, Ohio, and which is currently in the custody of law enforcement at 716 Middle Road, Conneaut, Ohio (the “Gateway Desktop”);
- b. a search warrant authorizing a search of one Huawei brand cellular phone, black in color, Model U3900, Serial No. BPGDYAA0022460790D9200; SNID A3E9K15307000191, which was recovered earlier today during the execution of a search warrant signed yesterday by this Court, from the person of Keith Seppi and which is currently in the custody of law enforcement at 716 Middle Road, Conneaut, Ohio (the “Keith Seppi Phone”);
- c. a search warrant authorizing a search of one Huawei brand cellular phone, red in color, with a marking “Consumer’s Cellular” on the outside, Model U3900, Serial No. A3E9K14B10002893, which was recovered earlier today during the execution of a search warrant signed yesterday by this Court, from the person of Donna Seppi and which is currently in the custody of law enforcement at 716 Middle Road, Conneaut, Ohio (the “Donna Seppi Phone”; collectively with the Gateway Desktop and the Keith Seppi Phone, the “Devices”);

for evidence identified in Attachment A to this application and search warrant, which are items evidencing violation of Title 18, United States Code, Section 844(d), which makes it unlawful to transfer and transport explosive materials in interstate commerce with the knowledge or intent that it will be used to kill, injure, or intimidate any individual.

4. Based on my training, knowledge and experience, and my discussions with other law enforcement officers, I know that the Devices have been stored in a manner in which their contents are, to the extent material to this investigation, in substantially the same state as they were when the Devices first came into the possession of law enforcement.

5. The applied-for warrant would authorize the forensic examination of the Devices for the purpose of identifying electronically stored data particularly described in Attachment A.

#### **BASIS OF INFORMATION**

6. The information contained in this Affidavit is based upon information gathered by me as a part of the investigation, as well as information provided to me by other law enforcement officers involved in this investigation. Because this affidavit is being submitted for the limited purpose of securing the above-requested search warrants, I have not included each and every fact known to me concerning this investigation. I have set forth only those facts that I believe are necessary to establish probable cause to believe that evidence of a violation of Title 18, United States Code, Section 844(d), as outlined in each of the proposed Attachments, will be found in the places for which search authority is being requested.

#### **DEFINITIONS**

7. This this affidavit and in the attachments, I refer to certain terms relating to computers and cellular phones. Those terms are defined below.

8. “Computer” refers to “an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device.” See 18 U.S.C. § 1030(e)(1).

9. “Computer hardware” consists of all equipment that can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including, but not limited to, central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes, and other memory storage devices); peripheral input/output devices (including, but not limited to, keyboards, printers, video display monitors, and related communications devices such as cables and connections); as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including, but not limited to, physical keys and locks).

10. “Computer passwords and data security devices” consist of information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alphanumeric characters) usually operates what might be termed a digital key to “unlock” particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software or digital code may include programming code that creates “test” keys or “hot” keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or “booby-trap” protected data to make it inaccessible or unusable, as well as reverse the process to restore it.

11. “Computer-related documentation” consists of written, recorded, printed, or electronically stored material that explains or illustrates how to configure or use computer hardware, computer software, or other related items.

12. “Computer software” is digital information that can be interpreted by a computer and any of its related components to direct the way it works. Computer software is stored in electronic, magnetic, or other digital form. It commonly includes programs to run operating systems, applications, and utilities.

13. “Internet Protocol address” or “IP address” refers to a unique number used by a computer to access the Internet. IP addresses can be dynamic, meaning that the Internet Service Provider (ISP) assigns a different unique number to a computer every time it accesses the Internet. IP addresses might also be static, if an ISP assigns a user’s computer a particular IP address that is used each time the computer accesses the Internet.

14. “Wireless telephone” refers to a wireless telephone (or mobile telephone, or cellular telephone), which is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional “land line” telephones. A wireless telephone usually contains a “call log,” which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic “address books;” sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones

may also include global positioning system (“GPS”) technology for determining the location of the device.

**PRIOR INVESTIGATION INTO THE BOMBING ON MAY 29, 2016**

29. This application is submitted in connection with an ongoing investigation into a bombing that occurred early in the morning on May 29, 2016, in which Alan P. Dobransky, a resident of Floyd, New York was severely injured when a package left at the end of his driveway exploded. On June 6, 2016, this Court issued search warrants, 4:16-MJ-6046; 4:16-MJ-6047; 4:16-MJ-6048; 4:16-MJ-6049; 4:16-MJ-6050; for the residences of Keith Seppi and Cindy Shields, for the pickup truck owned by Keith Seppi and for the person of Keith Seppi (the “June 6 Warrants”). ATF Agent Harry Maxwell submitted an affidavit in support of the applications for the June 6 Warrants (the “Maxwell Affidavit”). A copy of the Maxwell Affidavit is attached hereto as Exhibit 1. That affidavit sets forth relevant facts regarding the investigation and is incorporated by reference in this affidavit. Law enforcement executed the June 6 Warrants on June 7, 2016. In connection with the searches, law enforcement recovered the Devices. As explained in the Maxwell Affidavit and as set forth in more detail below, there is probable cause to believe that the Devices have evidence of a violation of Title 18, United States Code, Section 844(d).

**ADDITIONAL FACTS GATHERED**

30. Subsequent to the issuance of the June 6 Warrants, additional investigation has revealed more information establishing probable cause to believe that the Devices contain evidence of a violation of Title 18, United States Code, Section 844(d).

31. Law enforcement conducted an interview of Keith Seppi on June 7, 2016. Keith Seppi was advised of his *Miranda* rights, waived those rights, and agreed to speak with law enforcement. Keith Seppi disclosed the following:

- a. He admitted to making an explosive device in Ohio with the intent to deliver it to the residence of Alan Dobransky at 8219 Old Floyd Road, Floyd, NY;
- b. He admitted to personally transporting that explosive device, by driving his pickup truck from Ohio to Dobransky's residence; and
- c. He admitted to arming the explosive device.

32. Law enforcement also conducted an interview on June 7 of Donna Seppi, who is the wife of Keith Seppi and the sister of Cindy Shields. Donna Seppi was advised of her *Miranda* rights, affirmatively waived those rights, and agreed to speak with law enforcement. Donna Seppi disclosed the following:

- a. She was aware that her husband, Keith Seppi, had constructed an explosive device, transported it from Ohio to New York where he intended to detonate it in an effort to scare Dobransky;
- b. Her sister, Cindy Shields, was aware of Keith Seppi's plan with respect to the explosive device.

#### **THE GATEWAY DESKTOP**

33. The Gateway Desktop was recovered from a desk in the residence of Keith Seppi at 716 Middle Road. Investigators conducting the search of the residence were able to confirm that the residence has an Internet connection through a modem serviced by Dish Network.

34. I am aware from my training and experience, and my discussions with other law enforcement officers, that there is substantial information available on the Internet regarding the construction and use of destructive devices. I am also aware that Keith Seppi accessed the Internet and conducted searches for information relating to the construction of explosive devices.

In particular, and as explained in the Maxwell Affidavit, investigators viewed the publicly-available Facebook account of Keith Seppi, which had a post from February 8, 2016 titled, "TRIP-WIRE BANG HOME ALARM." The article posted from [www.diybullseye.com](http://www.diybullseye.com) provided instructions on how to build a home-made, outdoor trip-wire alarm using common household items, including a mousetrap, fishing line, (explosive) ring caps, nails, and screws. In my view, this post on Seppi's account shows an interest and proclivity for building home-made explosive devices.

35. In addition, as explained in the Maxwell Affidavit, the hotel clerk who identified Keith Seppi explained that Seppi handed the clerk printed-out directions in an effort to try to locate the victim's home address. This suggests that there may be information on the computer relating to Internet searches for the victim's address.

**KEITH SEPPI PHONE AND DONNA SEPPI PHONE**

36. Both Keith Seppi and Donna Seppi have admitted to being aware of the plot to transport an explosive device from Ohio to New York with the intent to detonate it. Donna Seppi has also confirmed that her sister was aware of the plot. As explained in the Maxwell Affidavit, toll records from Verizon Wireless suggest that there were numerous telephone calls from the telephone numbers associated with Keith Seppi and Cindy Shields during the times relevant to this investigation. Accordingly, there is probable cause to believe that both the Keith Seppi Phone and the Donna Seppi Phone contain evidence of a violation of Title 18, United States Code, Section 844(d).



**SPECIFICS OF SEARCHES OF COMPUTER AND  
WIRELESS COMPUTER SYSTEMS**

37. I have spoken with law enforcement personnel trained in computer evidence recovery that have knowledge about the operation of computer systems and the correct procedures for the seizure and analysis of computer systems.

38. These individuals have participated in the execution of numerous search warrants during which they have seized and/or examined computer systems. These individuals have also participated in several warrants that involved the search and/or seizure of, and has been responsible for analyzing, seized electronic data and records from those systems.

39. Based on my discussion with these individuals, plus common-sense knowledge, it is clear that in today's technological world computers and computer related media are used for communication and storage of data and information. As such, it is reasonable to believe that some or all of the records sought to be seized will be in electronic/digital format.

40. Based on my knowledge, training and experience, I know that electronic devices, such as the Device, can store information for long periods of time. This information can sometimes be recovered with forensics tools.

41. Furthermore, based upon my training, experience, and consultations with law enforcement personnel who specialize in searching computer systems, I have learned that searching and seizing information from computer systems and other storage media (including PDAs, cell phones, MP3 Players, etc.) often requires agents to seize most or all the computer system or storage media to be searched later by a qualified computer forensic examiner in a laboratory or other controlled environment. This is true for the reasons set out below.

42. The volume of data stored on many computer systems and storage devices will typically be so large that it will be highly impractical to search for data during the execution of the

physical search of the premises. The hard drives commonly included in mere desktop computers are capable of storing millions of pages of text; the storage capacity of other electronic devices (e.g. a micro drive, a thumb drive, etc.) can also be significant. Unlike the search of documentary files, computers store data in "files" that cannot easily be reviewed. For instance, a single 1 gigabyte of storage media is the electronic equivalent of approximately 500,000 pages of double spaced text. Most computer and electronic devices have capacities well in excess of a single gigabyte.

43. The search through the computer (or other electronic media) itself is a time consuming process. Software and individual files can be "password protected." Files can be placed in hidden directories; files can be mislabeled or be labeled with names that are misleading. Similarly, files that contain innocent appearing names ("Smith.ltr") can in fact be electronic commands to electronically cause the data to self destruct. Also, files can be "deleted," but, unlike documents that are destroyed, the information and data from "deleted" electronic files usually remains on the storage device until it is "over written" by the computer. For example, the computer's hard drive stores information in a series of "sectors," each of which contains a limited number of electronic bytes, usually 512. These sectors are generally grouped to form clusters. There are thousands or millions of such clusters on a hard drive. A file's clusters might be scattered throughout the drive (for example, part of a memo could be at Cluster 163, while the next part of the memo might be stored at Cluster 2053). For a non deleted file, there are "pointers" that guide the computer in piecing the clusters together. For a file that has been deleted, the "pointers" have been removed. Therefore, the forensic examination would include the piecing together of the associated clusters that made up the "deleted" file. Being aware of these pitfalls, the investigator/analyst must follow a potentially time consuming procedure to

review the contents of the computer storage device so as to insure the integrity of the data and/or evidence. A single computer and related equipment could take many days to analyze properly.

44. Computer storage media are used to save copies of files and communications, and printers are used to make paper copies of these communications and files. Applications and associated data stored on the storage media are the means by which the computer can send, print and save such activity. Finally, password protected data and other security devices are often used to restrict access to or hide computer software, documentation or data. All these parts of a computer are integrated into the entire operation of a computer. In order to evaluate the evidence most effectively, the computers and all of the related computer equipment described above should be available to a computer investigator/analyst.

45. Therefore, based upon my knowledge, training, and experience, as well as information related to me by Special Agents and others involved in forensic examination of computers, I am aware that searches for and seizures of evidence from computers commonly require Agents to seize most or all of a computer system's input/output and peripheral devices (including other storage media), in order for a qualified computer expert to accurately retrieve the system's data in a laboratory or other controlled environment. In order to fully retrieve data from a computer system, investigators must seize all the storage devices, as well as the central processing units (CPUs), and applicable keyboards and monitors which are an integral part of the processing unit.

46. Furthermore, searching computer systems is a highly technical process which requires specific expertise and specialized equipment. There are so many types of computer hardware and software in use today that it is rarely possible to bring to the search site all of the necessary technical manuals and specialized equipment necessary to conduct a thorough search. In addition, it may also be necessary to consult with computer personnel who have specific

expertise in the type of computer, software application or operating system that is being searched.

47. The best practices for analysis of computer systems and storage media rely on rigorous procedures designed to maintain the integrity of the evidence and to recover hidden, mislabeled, deceptively named, erased, compressed, encrypted, or password protected data while reducing the likelihood of inadvertent or intentional loss or modification of data. A controlled environment, such as a law enforcement laboratory, is typically required to conduct such an analysis properly.

#### **SEARCH METHODOLOGY TO BE EMPLOYED**

48. As further described in Attachment A, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the Device was used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the Device because:

- a) Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).
- b) Forensic evidence on a device can also indicate who has used or controlled the device. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence.
- c) A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to

draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

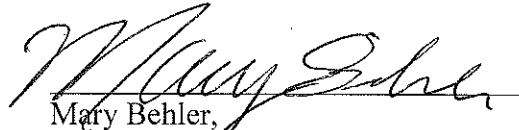
49. The search procedure of electronic data contained in computer hardware, computer software, and/or memory storage devices may include the following techniques (the following is a non-exclusive list, as other search procedures may be used):

- a) on-site triage of computer systems to determine what, if any, peripheral devices or digital storage units have been connected to such computer systems, as well as a preliminary scan of image files contained on such systems and digital storage devices to help identify any other relevant evidence or potential victims;
- b) examination of all of the data contained in such computer hardware, computer software, or memory storage devices to view the data and determine whether that data falls within the items to be seized as set forth herein;
- c) searching for and attempting to recover any deleted, hidden, or encrypted data to determine whether that data falls within the list of items to be seized as set forth herein (any data that is encrypted and unreadable will not be returned unless law enforcement personnel have determined that the data is not (1) an instrumentality of the offenses, (2) a fruit of the criminal activity, (3) contraband, (4) otherwise unlawfully possessed, or (5) evidence of the offenses specified above);
- d) surveying various file directories and the individual files they contain;
- e) opening files in order to determine their contents;
- f) scanning storage areas;

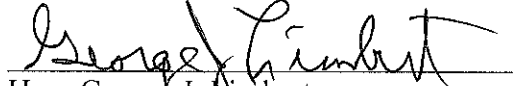
- g) performing key word searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are likely to appear in the evidence described in Attachment A; and
- h) performing any other data analysis technique that may be necessary to locate and retrieve the evidence described in Attachment A.

**CONCLUSION**

50. Based upon the above information, I respectfully submit there is probable cause to believe that evidence of a violation(s) of Title 18, United States Code, Section 844(d) will be found within the Devices. Accordingly, I respectfully request that this Court issue the requested search warrants, and authorize the search for evidence as particularly described in the respective proposed Attachment to each of the corresponding search warrants being sought by this Application.

  
Mary Behler,  
Senior Special Agent, ATF

Sworn and subscribed before me  
this 7 day of June, 2016.

  
Hon. George J. Lambert  
United States Magistrate Judge